**STATEMENT OF**
**JACQUELYN L. WILLIAMS-BRIDGERS**
**INSPECTOR GENERAL OF THE**
**U.S. DEPARTMENT OF STATE,**
**ARMS CONTROL AND DISARMAMENT AGENCY, AND THE**
**UNITED STATES INFORMATION AGENCY, INCLUDING**
**INTERNATIONAL BROADCASTING**

**FOR THE**

**COMMITTEE ON GOVERNMENT REFORM**
**SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND**
**INTERNATIONAL RELATIONS**
**U.S. HOUSE OF REPRESENTATIVES**

**FEBRUARY 25, 1999**

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to testify before your subcommittee on the major management challenges facing the Department of State. As my office also oversees the United States Information Agency (USIA), including international broadcasting, and the Arms Control and Disarmament Agency (ACDA), my testimony will incorporate some management challenges that apply to all three agencies.

## Summary

My office has identified several significant challenges facing the agencies that we oversee. Foremost among these is the safety and protection of our people, facilities, and information. The scope and gravity of this challenge was brought into clear focus by the attacks on U.S. embassies in Africa last year. The Department is faced with the immediate need to address physical security vulnerabilities and enhance emergency planning at our overseas posts. Longer-term challenges include major embassy renovations to improve security, new embassy construction, and the maintenance of security equipment.

Another critical challenge facing the foreign affairs agencies is their vulnerability to the Y2K problem. Generally, the Department is making steady progress toward preparing computer systems for the Year 2000 date change, and estimates that 55 of 59 mission-critical systems will be implemented by the Office of Management and Budget's (OMB's) March 31, 1999 deadline.

Despite this progress, we are concerned that the Department's Y2K certification process, which is designed to provide documented independent assurance that all possible

steps have been taken to prevent Y2K-related failures, is proceeding too slowly. Thus far, only two mission-critical systems have been certified by the Department's Y2K Certification Panel. Failure to meet the Y2K challenge could create havoc in the foreign affairs community, including disruption of messaging systems, impediments to embassy operations such as visa and passport processing, and failures in administrative functions such as payroll and personnel processing in the Year 2000.

I would also like to share with you some of our observations of the Department's planning process and implementation of the Government Performance and Results Act (Results Act). Although strategic planning efforts as required by the Results Act have prompted some improvements in the Departments planning process, more measurable goals and outcomes are needed.

Other major challenges faced by the Department include the need to strengthen border security, consolidate the foreign affairs agencies, correct weaknesses in financial management and improve real property management and maintenance. Before I provide additional details on these challenges, I would like to give you a sense of OIG's mission and responsibilities, as well as provide a brief overview of our strategic plan.

## OIG Operations

### OIG Organizational Structure

The mandate of my office is to improve the economy, effectiveness, and efficiency of the Department of State (the Department), ACDA, USIA, and the Broadcasting Board of Governors and to detect and prevent waste, fraud, and mismanagement. Toward this end, OIG consists of four operational offices that carry out inspections, audits, and investigations.

Office of Audits. OIG's office of Audits consists of seven divisions, each with a specific area of focus: Consular and International Programs, Information Management, Financial Management, Property Management and Procurement, International Broadcasting, Human Resources, and Contracts and Grants. Audits conducted by these divisions assess management and financial operations and the economy or efficiency with which an entity is managed. Examples of reviews the Office of Audits is currently conducting include the Department's Consular Fraud Program, Year 2000 (Y2K) remediation efforts, implementation of the International Cooperative Administrative Support Services (ICASS) system, management of overseas property, and financial statement preparation.

Office of Inspections. OIG is required by law to routinely inspect the activities of overseas posts and domestic bureaus. These inspections are conducted to provide overseas missions and domestic bureaus information about the effectiveness of their performance and the quality of their management and operations through an assessment of three primary areas: policy implementation, resource management,

and management controls. In FY 1998, the office inspected posts in 32 locations, including Russia, China, Thailand, and several African countries.

Office of Security and Intelligence Oversight. Through audits and inspections, the Office of Security and Intelligence Oversight evaluates the ability of overseas posts to respond to threats from terrorism, mobs, or other physical intrusion, intelligence penetrations, and crime through audits and inspections. The office also evaluates whether the Department's security and intelligence programs and activities are being carried out with the most effective use of resources and in accordance with the law. Our security oversight inspection program supports the Secretary of State's statutory responsibility for the security of all nonmilitary U.S. personnel, property, and information abroad.

In an effort to add greater rigor to OIG's intelligence oversight responsibilities, I created an Intelligence Oversight Division within the Office of Security and Intelligence Oversight. The division reviews foreign policy aspects of programs and functions involving components of the intelligence community and identifies key areas of concern in the review of intelligence oversight and coordination by chiefs of mission.

Office of Investigations. The Office of Investigations performs investigations of criminal, civil, and administrative misconduct related to organizational programs and operations. Additionally, the office manages a Hotline for employees who wish to disclose potential fraud, waste, and mismanagement. The office also focuses on fraud prevention by increasing employee awareness and understanding of the standards of conduct and accountability and by reducing areas of vulnerability and opportunities for misconduct. We publish "Standards of Conduct," a guide to ethical conduct, which is issued to each employee in the Department, USIA, and ACDA. My office also issues fraud alert bulletins and management implication reports when our work identifies systemic weaknesses that have agency-wide or bureau-wide implications.

## Followup and Resolution

Once an OIG report is issued, Department bureaus or posts with responsibility for implementing the report's recommendations have 45 days in which to respond. The responses are reviewed by OIG to determine whether they meet the intent of the recommendation. In the event that the bureau or post does not accept the recommendation as written, OIG can either accept the suggested alternative, if any, or refer the decision to the next management level for reconsideration. If an impasse is reached in resolving a recommendation, it is referred for decision to the Under Secretary for Management or, ultimately, to the Secretary of State or agency director.

The OIG semiannual report to the Congress identifies audit significant recommendations unresolved or outstanding during the 6-month review period. In

addition, the Secretary or agency Director is required to report to the Congress twice each year on any recommendations for which resolution has not been achieved within a year. Our most recent semiannual report shows outstanding OIG recommendations in areas identified as management challenges, including maintenance and repair of buildings overseas, financial system acquisition and development, mainframe systems security, and management of secure communications.

OIG Strategic Plan

The Secretary of State has established seven broad national interests and strategic goals for international affairs in the following areas: National Security, Economic Prosperity, Enhanced Services to American Citizens overseas and Controlling U.S. Borders, Law Enforcement, Democracy, Humanitarian Response, and Global Issues. The Secretary's National Interests provide the framework within which the OIG conducts its integrated program of audits, inspections, and interdisciplinary reviews to evaluate progress toward achieving the Secretary's objectives.

OIG's strategic plan establishes the OIG-wide goals that guide the work we will undertake into the 21st century. OIG strives to be proactive in addressing foreign affairs agencies' efforts to effectively implement U.S. foreign policy; clearly link resources to policy objectives; and maintain efficient, effective, and secure operations and infrastructures. We are committed to protecting the Secretary of State's ability to pursue the foreign policy objectives of the United States free from the impediments of waste, fraud, and mismanagement.

I would like to turn now to a more detailed discussion of the major management challenges facing the Department in the context of OIG strategic objectives.

## Improved Implementation of Foreign Policy

The successful development and implementation of U.S. foreign policy depends on many factors. These include a clear understanding of foreign policy goals, coordination among the various agencies and entities with foreign policy interests, and clear and consistent lines of communication between the President, the Secretary of State, and the internal components of the Department.

Strengthening Border Security

Over the past few years, the Department has maintained a strong emphasis on the need to improve border security, however, the passport process and the immigrant and nonimmigrant visa processes remain material weaknesses. Improvements needed to address these weaknesses include additional management positions to support consular automated systems, expanded intelligence information sharing among U.S. Government agencies, and the installation of modernized machine-readable visa systems worldwide. In terms of consular staffing, our own work has shown that the Department will face

severe shortages of experienced midlevel managers for the next several years. We have also pointed out the need for more senior, experienced consular officers at posts with high fraud levels.

The Department has mounted a major effort to counter visa fraud, including initiatives such as the machine-readable visa program, worldwide advisories to overseas posts on detecting fraudulent documents, and programs to detect terrorists. The Department also continues to refine its consular lookout systems to identify names with different spellings or those that may be translated into multiple spellings. This will better enable the Department to identify individuals who should not receive visas. OIG is currently reviewing the Department's consular fraud prevention efforts to evaluate several aspects of the program, including the adequacy of the Department's guidance and training in fraud prevention and the coordination of antifraud efforts.

Our work in this area has facilitated several improvements in the Department's consular operations. For example, our recommendations helped ensure that the modernized version of the machine-readable visa system has the capability to electronically transmit relevant data on visa issuances to the Interagency Border Inspection Service for transmission to ports of entry. Also, our work encouraged the Department to establish a proactive program to identify individuals ineligible for a nonimmigrant visa in its computer system, such as drug traffickers, alien smugglers, and organized crime members. Additionally, an OIG recommendation contributed to the Department's ensuring that consular officers overseas have access to information on individuals from high-risk countries listed on the Department's CD ROM.

OIG also recently reviewed the U.S. border crossing card replacement program for eligible citizens of Mexico. The laser visa is more tamperproof than previous documents. However, many problems reduce the effectiveness of the program, such as the lack of laser visa processing equipment at consular posts in Mexico, an inadequate criminal database against which to check applicants, delays in production, and continued issuance of nonbiometric 10-year visas. Because the Department is not solely responsible for implementing this program with other agencies, a multi-agency effort will be needed to address many of these issues. The problems identified jeopardize the timely implementation of the program and compromise its enhanced border security protection.

## Better Alignment of Fiscal and Human Resources with U.S. Foreign Policy Priorities

The Results Act requires Federal agencies to set goals for program performance and to measure results with the goal to improve the efficiency and effectiveness of Federal programs. Specifically, the law requires that each agency submit to Congress and OMB a 5-year strategic plan for program activities. The plan is to contain goals and objectives, and how they will be achieved. Each agency is also required to submit an annual performance plan with measurable goals and indicators that link to the strategic plan.

Over the past three years, strategic planning efforts as required by the Results Act have prompted notable improvements in the Departments planning process. For example, at posts overseas there is increased focus and discussion on the U.S. Government's overall goals in each country. Also, there is an improved collective assessment of all U.S. Government resources available at each post to achieve specific mission goals.

The challenge that exists for the Department and its partners in the foreign affairs community is to define goals stated in mission, bureau, and Department plans in more measurable terms, and in terms of outcomes--what the U.S. hopes to achieve--rather than broad policy statements. In addition, the Department needs to establish a credible system that will allocate resources across geographic boundaries.

The upcoming merger of foreign affairs agencies will provide an opportunity to realign foreign affairs resources with policy priorities. Effective integration of the foreign affairs agencies will depend, in large part, on the success of merging diverse personnel systems, adapting varied and diverse information systems, and melding complex financial systems.

Linking Resources to Foreign Policy Priorities

In response to changing foreign policy priorities, and the need to demonstrate positive outcomes, the Department developed a strategic plan containing 16 international affairs strategic goals and 3 diplomatic readiness goals. The Department then asked each post and bureau to submit a plan and budget linked with the Department's strategic goals. At the request of the Department, OIG has been active in reviewing the mission and bureau planning process.

Mission Performance Plans are the principal vehicle for documenting and reaching interagency consensus on country-level goals and strategies. The Mission Program Plans, in turn, serve as building blocks for the Bureau Performance Plans, and ultimately, the Department's budget submission to OMB. However, OIG found that the process used during FY 1998 to develop Mission Performance Plans was poorly timed, and the guidance sent to the Bureaus and posts was unclear. The unclear guidance resulted in some incomplete or incorrect plans, and performance indicators that did not necessarily link with the indicators, baselines and targets included in the Department's overall performance plan. Further, the software intended to link budgets with goals and objectives, the Resource Allocation and Budget Integration Tool proved cumbersome, ineffective and difficult to deploy, and the Department is currently developing a new system to replace it. These problems resulted in corresponding weaknesses in the Bureau Performance Plans.

To date, the Department has been unsuccessful in implementing Results Act requirements for performance plans. The Department's FY 1999 Performance Plan, which was developed from the Bureau Performance Plans, did not comply with the

Results Act, and both Congress and the Department identified several deficiencies with the plan. For example, the plan lacked baselines and performance targets, omitted management initiatives, contained goals that were broadly stated and extended beyond the Department's span of control, and provided little information on the resources required to achieve specific performance goals.

Although the draft of the combined FY 1999-2000 performance plan still does not comply with the Results Act, it is an improvement over the previous plan. For instance, the Department decided to focus its initial attention on the management bureaus, and as a result, the plan contains a comprehensive set of performance goals, baselines, and targets for the Department's diplomatic readiness goals. However, the sections in the plan on the 16 strategic goals are incomplete, providing only one illustrative goal paper under each strategic goal. For example, under the strategic goal on regional security, the Department provides a performance goal, indicators, baselines, and targets only for its efforts in Northern Ireland.

OIG will continue to assess the Department's progress in implementing the GPRA, and will take steps to verify and validate selected performance data. In addition, our audits will include reviews of the performance measures related to the areas reviewed. For example, our review of Foreign Trade Barriers will determine whether the Department's FY 1999 performance goals, indicators, and information sources accurately reflect its progress in opening foreign markets in the telecommunications industry.

The International Cooperative Administrative Support Services (ICASS) system was initiated in 1996 in response to a congressional mandate to implement a system that allocates to each department and agency the full cost of its presence abroad. Additionally, ICASS was intended to provide posts more control of administrative services through local empowerment, equity, transparency, local selection of service providers, and the establishment of customer service standards. The goal was to obtain quality services at the lowest cost. OIG initiated a review of the ICASS program to assess posts' progress in selecting the most cost-effective service providers.

Our work to date has generally shown that posts have not yet used ICASS to seek out more cost-effective service providers. There are a number of reasons for this: the process for selecting alternate providers is unclear, post ICASS councils lack training and expertise in selecting alternate service providers, and the Department and ICASS Councils lack the authority to mandate that other agencies participate in what may be the most cost-effective solution for the U.S. Government through economies of scale.

At some posts, a few agencies have opted out of ICASS services. While those agencies have reported reducing their operating costs from what ICASS charges, the total U.S. Government costs may be higher since costs were redistributed among the agencies that did not opt out and ICASS staffing levels remained the same. We also found that some posts have not fully implemented ICASS, and ICASS information is not being used within Department headquarters elements to seek out more cost-effective alternatives.

Consolidating Foreign Affairs Agencies

The Omnibus Consolidated Appropriations and Emergency Supplemental Appropriations Act for FY 1999 mandated the consolidation of the Department of State, the Arms Control and Disarmament Agency, and the United States Information Agency into one foreign affairs agency.

OIG is addressing consolidation issues on a number of fronts. In a review conducted prior to the legislation merging the foreign affairs agencies, OIG recommended the consolidation of the security function in USIA and the Department. We determined that USIA's Office of Security could be merged with the Department's Bureau of Diplomatic Security resulting in more streamlined security activities. We identified about $500,000 in funds that could be put to better use, including up to 10 positions that could be used for other purposes in the security area. USIA's security staff will be formally integrated in October 1999 into the Department's Bureau of Diplomatic Security pursuant to the recent omnibus appropriations legislation.

The merger of the foreign affairs agencies also raises several challenges in the area of personnel management. Numerous policies and practices that differ between the Department and USIA such as assignment procedures, language training, tenuring regulations, and Senior Service competition rules will have to be reconciled. The Department has stated its intention to offer increased opportunities for retraining and upgrading employee skills and to work with USIA staff to integrate public diplomacy into the curriculum at the Foreign Service Institute.

Overseas tours of duty are another example where personnel policies differ between agencies. The Department's current policy of two- and three-year tours for staff at virtually all overseas posts differs from other government agencies, including USIA, where the tour is four years. A recent OIG review found that longer tours would reduce costs, and increase employee productivity. Costs could be reduced because longer tours would reduce the number of times employees move--the average cost of a move was over $18,000 in fiscal year 1996. Also, because of the considerable time necessary to become oriented to a new post, and the time at the end of the tour to bid for and transfer to the next post, longer tours would increase the time employees were fully productive in their current position.

Several studies by the Department and other groups have also recommended lengthening tours to improve effectiveness and achieve cost savings. However, in January 1999, Department officials announced that they would apply the Department's tour length policy when the foreign affairs agencies are consolidated, rather than adopt longer tours. In our view, this is a missed opportunity for the Department to increase the effectiveness of overseas personnel while also achieving cost savings.

The consolidation of foreign affairs agencies also presents a challenge to incorporate the best use of technology by USIA into the Department. The Department faces the challenge of effectively merging its decentralized information resources management organization with USIA's highly centralized system -- at a time when both agencies are working to resolve Y2K problems in their respective systems. In addition, connecting USIA systems to Department systems must take into account necessary security considerations.

The pending merger of USIA and the Department has raised the issue of whether USIA's Y2K certification efforts meet the stringent standards set by the Department. USIA's current certification process is of concern for two reasons. First, it lacks independent verification of Y2K compliance because the same contractor is tasked with both remediation and validation. Second, USIA's certification guidelines do not contain the level of detail and specificity used by the Department. When USIA merges with the Department in October 1999, USIA functions and the systems that support those functions will become the Department's responsibility. As such, we believe it would be prudent for the Department to assure itself that USIA's systems are evaluated for Y2K compliance on the same basis as Department systems.

Financial management challenges are also associated with the consolidation of foreign affairs agencies. This includes integrating USIA and ACDA into the Department's Central Financial Management System, which is being upgraded. The preparation of accurate and timely agencywide financial statements which include data from each agency will be necessary. Complicating the process is the fact that neither ACDA nor USIA is currently required to prepare audited financial statements under the Government Management Reform Act.

The consolidation of the Department and ACDA is planned to occur during FY 1999; therefore, ACDA will be included in the Department's FY 1999 financial statements. Because ACDA is a fairly small agency in relationship to the Department, no significant problems are expected from the consolidation of the financial information. The consolidation of financial information with USIA is more significant and complicated. The Department and USIA plan to consolidate on October 1, 1999, which means the consolidated information would be reflected in the FY 2000 financial statement. However, to facilitate the preparation of the consolidated statements, as well as provide a proper accounting of assets to be transferred to Broadcasting Board of Governors, USIA should, at a minimum, prepare an audited statement of its financial position for FY 1999.

**More Effective, Efficient, and Secure Operations and Infrastructures**

The ability of the State Department, ACDA, and USIA to advance the foreign policy interests of the United States and their respective missions depends upon the quality of agency operations and infrastructure. Readiness to promote national interests and represent the United States to the world requires high-performance organizations with efficient and effective supporting systems.

As demonstrated by the terrorist attacks on U.S. embassies in Nairobi and Dar es Salaam, perhaps no greater challenge exists for the Department than providing adequate security to protect our people, facilities, and information. In response to the bombings, the Department is aggressively addressing physical security vulnerabilities and enhancing emergency planning at our overseas posts. I have also taken a number of steps to significantly enhance the security oversight operations of my office.

The foreign affairs agencies also face challenges in other areas related to operations and infrastructures. Generally, the Department is moving ahead on preparing computer systems for the Year 2000 date change, and expects to have the majority of its mission-critical systems implemented by the OMB deadline of March 31, 1999. Despite this progress, we are concerned that the Department's Y2K certification process is proceeding too slowly.

In the area of financial management, the Department's financial and accounting systems are inadequate, and there are significant concerns with the security of financial systems on the Department's mainframe computer systems. In property management, the Department has yet to establish a baseline of maintenance and repair requirements and costs for overseas property.

Addressing Security Vulnerabilities

The bombings of U.S. embassies in Nairobi and Dar es Salaam underscored the vulnerability of some of our posts and changed the approach to security at our missions for both the Department and OIG. Prior to the bombings in Africa, the Department generally allocated security resources to overseas posts based on the threat category of the city in which the diplomatic facility was located. The Department gathered threat information from a variety of sources and published a classified "Composite Threat List." Threats fell into four categories: political violence, human intelligence, technical intelligence, and crime. Threat levels in each of these categories ranged from critical to low. Embassies with a "critical threat" rating were generally allocated more funds for security enhancements than those embassies with "low threat" ratings. The bombings of our embassies, however, have caused the Department to realize that allocating resources based solely on the use of the Composite Threat List is inadequate. In addition to the threat rating, the Department now factors in the vulnerability of all posts to terrorist attacks. Under this new approach, all posts should meet a high level of protection against acts of terrorism and political violence.

In response to the attacks on our embassies last year, the Department conducted an extensive review of mission security around the world and identified eight facilities so vulnerable that the missions will be moved into safer, more secure facilities as quickly as possible. In Nairobi, the mission is moving into interim office buildings that will provide a degree of security until new office buildings can be constructed and occupied. In Dar es Salaam, such a move has already taken place. Construction of new embassies in these countries is scheduled to be complete by 2003. The Department also plans to undertake significant renovations to address serious vulnerabilities at other locations. For example, the Department plans to enlarge the setback at one post at a cost of $21 million.

To enhance emergency response, the Department plans to spend $118 million on handheld radios. This will serve to upgrade the entire emergency radio program and send new radios to every overseas post for use during an emergency. The Department is also planning to purchase satellite telephones so that posts and emergency response teams can depend on reliable communication during and after an emergency.

Staffing shortages in security have been addressed by the recent supplemental appropriation, and the Department is engaged in an aggressive recruitment program for both security officers and security engineers to increase its workforce. However, the training period in the Department before new security officers gain the expertise to perform successfully overseas has historically taken up to 6 years. The new officers will be going overseas with only 2 or 3 years of experience. To examine the adequacy of the Department's support of these new officers, we plan to review the Bureau of Diplomatic Security's overseas operations management in the coming year.

I have taken a number of steps to significantly enhance the security oversight operations of my office. First, we have expanded our security oversight inspections to include low and medium threat posts. Also, routine post management inspections now include an experienced security officer who focuses on physical security and emergency preparedness, and prepares a classified security annex to the inspection report. This year we plan to complete 16 security inspections, and to have our security officers accompany routine inspection teams to 15 additional posts. We also will complete security audits of the card access control program, protective details, the protection of classified information, and overseas telephone security.

Second, our new Security Enhancements Oversight Division will provide oversight of the $1.4 billion in emergency security funds, and future funding received by the Department, to enhance overseas security. OIG will evaluate physical and technical security being built into the new office buildings in Nairobi and Dar es Salaam. In addition, OIG will examine security for construction personnel, on-site construction, logistics for items used in the controlled access areas, and contract management. This Spring, an inspection team will evaluate the security at the interim office building in Dar es Salaam and the temporary office building in Nairobi.

Because a large portion of the emergency supplemental funds will go toward procuring goods and services and the construction of new facilities, OIG plans to provide audit assistance to ensure that contract costs are reasonable. OIG may audit selected contractors prior to award and at contract completion, and provide technical support to Department contracting officers in reviewing contractor proposed costs.

OIG already provides oversight of the embassy construction project in Moscow, Russia. The Moscow Oversight Team, established in 1994, provides oversight to the Moscow chancery construction project. The team was formed in response to the costly security mistakes that characterized previous construction efforts of Embassy Moscow. Rather than waiting to identify problems after the construction is complete, we have undertaken this ongoing oversight effort in order to flag potential vulnerabilities so that they can be addressed promptly. With this approach we are contributing our expertise to facilitate project completion on time, within budget, and in a secure manner.

Another important oversight project for OIG will be the China 2000 initiative, which is scheduled to enter the design phase in FY 1999. The Department will have to respond to several formidable challenges in order to construct secure compounds. Construction security oversight is critical to ensuring that the China 2000 project adequately addresses security needs, and that security systems, once designed, will function as intended.

Followup on Security Recommendations

For several years, my office has reported that the Department faced significant challenges in managing and funding security and made numerous recommendations to address specific vulnerabilities at our missions worldwide. The Department has generally corrected deficiencies identified by OIG where they have had resources available to do so. Of the 588 security recommendations made in FY 1997, the Department agreed to correct approximately 90 percent of the deficiencies and completed action on about 50 percent within one year after they were identified.

However, many of the recommendations still outstanding are significant, and require major capital investments to implement. Examples include relocating missions to safer facilities, building safe havens, or improving walls that surround the facility. Despite the recent emergency appropriation, the Department continues to face funding shortfalls. Security equipment will also need long-term funding. An OIG audit of the maintenance and repair of security equipment found that, despite the fact that much of the Department's equipment, purchased in the mid-1980's, was reaching the end of its useful life or was obsolete, the Department had not budgeted for new equipment.

OIG's audit of overseas card access systems found similar problems with equipment maintenance. The Department lacked a uniform program for the installation, repair, and maintenance of the card access system equipment. In addition, the equipment was never certified for use and, in some cases, was locally procured and maintained. We

have serious reservations as to whether the card access control systems can effectively control access and protect sensitive information. Our security inspections have repeatedly demonstrated that security at "lock-and-leave" posts without 24-hour cleared U.S. Marine Guard protection is often inadequate to protect classified material.

Emergency Preparedness

As a result of our audit on emergency evacuation, the Department reinstated its crisis management exercise program, which trains emergency action committees at posts on how to manage crises more effectively. The ability of posts to respond to emergencies, such as natural disasters or terrorist attacks, is greatly enhanced by the Department's crisis management exercises and emergency drills. However, our security inspections consistently report that posts are not conducting the required drills needed to prepare for likely attacks. In addition, we recently reported to the Bureau of Diplomatic Security on specific steps it should take to enhance procedures for vehicle bomb drills and coordinate with the Accountability Review Board, which addressed this in its report. In this respect, security inspection teams recommend regular practice of "duck and cover" drills along with specific recommendations for immediately alerting staff to vehicle bomb attacks.

Strengthening Information Security

The Department faces significant challenges in information systems security. Our work has pointed out deficiencies in the Department's mainframe and communication systems security, including incomplete and unreliable security administration, inadequate training, and lack of access control. Similar problems have been identified in specialized telephone switching and card access computer systems. In many cases, the Department is modernizing systems without a parallel effort to improve information security. A May 1998 General Accounting Office audit report reiterated our findings on the need for improved management of information security.

The Department also does not have sufficient backup capability at major data-processing facilities for use in an emergency; an issue raised by several OIG audits since 1989. The Department is in the process of developing a mainframe contingency program to provide an alternate processing site in the event of an existing system failure. OIG has stated that those backup sites and systems currently in place will not be effective until issues including planning, coordination, training and resources are resolved. In addition, once established, the contingency plans will need to be tested to ensure they work as planned.

Open OIG recommendations in the area of information security call for the Department to establish a security program for the mainframe system to address risks identified by OIG and to ensure that responsible officials are identified and kept informed about the systems security. We have also recommended that the Department require personnel who hold positions with access to bulk quantities of sensitive information to

undergo a special counterintelligence screening process prior to each assignment. This last issue will be the subject of an OIG audit scheduled to begin next month.

Achieving Y2K Compliance

Another critical challenge facing the foreign affairs agencies is their vulnerability to the Y2K problem. Generally, the Department is making steady progress toward ensuring that it is ready for the Year 2000 date change. As of February 8, 1999, the Department reported that 36 of 59 mission-critical systems had been fully implemented, and it expects to have 55 mission-critical systems implemented by the March 31, 1999, OMB deadline. Despite this progress, we are concerned that the Department's Y2K certification process, which is designed to provide documented independent assurance that all possible steps have been taken to prevent Y2K-related failures, is proceeding too slowly. Thus far, only two mission-critical systems have been certified by the Department's Y2K Certification Panel.

Failure to meet this challenge could create havoc in the foreign affairs community, including disruption of messaging systems, impediments to embassy operations such as visa and passport processing, and failures in administrative functions such as payroll and personnel processing in the Year 2000. The Department's presence at more than 260 locations worldwide increases the Department's challenge to continue functioning effectively in the Year 2000. Embassies and consulates rely on their respective host countries' infrastructures to provide essential, day-to-day services such as power, water, telecommunications, and emergency services. In some countries these services could be disrupted if critical infrastructure components and control systems are not made Y2K compliant.

My office has been actively engaged in Y2K efforts in three major areas. First, we assisted the Department in its efforts to develop certification guidelines identifying what steps the Department must take to determine whether systems are Y2K compliant, and identified documentation needed to certify computer systems as "Year 2000 ready." OIG is also evaluating the adequacy of certification packages prepared by bureaus for mission-critical systems. Second, we are reviewing Department and USIA efforts overseas to prepare adequately for the millennium change. This effort includes monitoring efforts of our overseas posts to raise global awareness of the Year 2000 problem, ensuring that U.S. embassy and consulate system vulnerabilities are properly addressed, and reviewing post contingency plans. Finally, because U.S. embassies and Americans living and working abroad might be vulnerable to Y2K-related infrastructure failures, we are assessing the Y2K readiness of host countries where the U.S. Government maintains a presence.

Our work with the Department has resulted in several improvements. A clearer definition of what constitutes "Y2K compliant" resulted in more accurate reporting to the Office of Management and Budget on the status of the Department's Y2K effort. OIG findings also resulted in greater focus on Departmentwide project management tracking;

discovery of seven new applications, which were added to the Department's system-tracking database; and development of a new rating system that tracks and evaluates system interfaces.

OIG has conducted site assessments in 25 cities in 20 countries as part of an aggressive effort to review embassy preparedness and collect and analyze information on host country Y2K efforts. Early on, OIG found little contingency planning at posts in the event of a failure of basic infrastructure services on January 1, 2000. The Department is aware of this problem, and is sending a Contingency Planning Toolkit to all embassies and consulates to assist them in developing their respective plans.

In our effort to assess the readiness of host countries to address Y2K-related problems, OIG has met with representatives from foreign governments, key infrastructure sectors, and private industry in each country we visited. We have provided information summaries on each of these countries to the Department, USIA, the President's Council on the Year 2000 Conversion, congressional committees, and other foreign affairs organizations.

OIG has initiated a series of USIA Worldnet Interactive broadcasts throughout Latin America and Canada. In coordination with the Organization of American States and USIA, these interactive programs have been broadcast live throughout this hemisphere and worldwide via the internet to explore problems, strategies and solutions in the areas of timely contingency planning, energy and financial institutions readiness, and auditing techniques to promote Y2K compliance.

Correcting Weaknesses in Financial Management

Financial management continues to be another major challenge facing the foreign affairs agencies. The Department accounts for more than $5 billion in annual appropriations and over $16.7 billion in assets. The Department has made significant improvements in financial management since the Chief Financial Officer's Act was passed in 1990. OIG has focused on the Department's financial management through our audits and annual review of the Department's progress to improve material weaknesses in conjunction with the preparation of the Federal Manager's Financial Integrity Act (FMFIA) report. Over the past few years, the Department has complied with OIG recommendations in areas such as disbursing, cashiering, travel advances, and accounts receivable, which significantly improved these areas and led to these weaknesses being removed from the FMFIA report.

However, a number of significant concerns still exist, some of which have been outstanding for a number of years. Although OIG's audit of the Department's 1997 agencywide financial statements showed that the Department's statements were free of material misstatements, the report brought to management's attention significant concerns with the security of the Department's domestic main frame computer.

OIG's audit of the Department's 1997 agencywide financial statements also raised concerns about the inadequacy of the Department's financial and accounting systems, which is both an internal control weakness and an issue of noncompliance with several laws and regulations, including the Federal Financial Management Improvement Act (FFMIA). The FFMIA requires that agencies report whether the Department's financial management systems substantially comply with the Federal financial management system requirements, applicable accounting standards, and the United States Standard General Ledger at the transaction level. Based on our review, OIG found that the Department does not substantially comply with one aspect of the FFMIA, that is the Federal financial management system requirements. The Department has reported its financial systems as a high-risk area and a material nonconformance for more than 15 years in its annual FMFIA report.

OIG has urged the Department to focus attention on its financial systems and to develop benchmark performance indicators to measure the improvements to these systems. In response to our recommendations, the Department is planning to study the level of compliance with the FFMIA and to prepare a remediation plan as required by that Act. The Department also has efforts underway to improve these systems, including upgrading its Central Financial Management System and developing standard financial capabilities for overseas posts.

Issues regarding timeliness of the financial statements and data, internal controls over major processes, and presentation of data for new requirements have yet to be resolved. OIG's last two audits of the financial statements identified the inadequacy of internal controls over the management of unliquidated obligations. Although we have recommended that the Department focus on this area, our preliminary audit work on the Department's 1998 financial statements shows that these weaknesses persist.

In addition, we have recommended that the Department ensure that adequate resources are devoted to financial statement preparation, especially during the preparation of the FY 1998 financial statements due to the increased reporting requirements. Based on our preliminary work, however, we have found that the Department is still unable to provide certain financial documentation by the agreed upon deadlines.

Grants management is another area of financial management weakness in USIA, and needs to be carefully considered in the consolidation with the Department. USIA annually awards about 500 domestic grants and cooperative agreements totaling approximately $240 million, about 1500 overseas grants totaling about $20 million, and numerous transfers to bilateral commissions and foundations totaling $120 million. OIG's audits have identified unauthorized, unallowable, and unsupported costs, internal control weaknesses, or noncompliance with applicable regulations associated with these awards. For example, OIG identified about $1 million in surplus funds at the Fulbright commission in India. USIA fully implemented our recommendation to offset the commission's 1998 allocation resulting in a one-time cost savings. Screening and monitoring of the recipients of these funds will become more critical because under

revised Office of Management and Budget guidelines, the majority of USIA's grantees will no longer be required to have annual financial audits.

Overall, Federal assistance funds in the form of grants, cooperative agreements, transfers, or loans from the Department, USIA, and ACDA total over $1 billion annually. For example, the Department's migration and refugee assistance programs alone amounted to $650 million in FY 1998. The Department is currently considering alternatives to managing grant activities once consolidation occurs.

Improving Real Property Management and Maintenance

Currently the Department reports holding 12,000 properties with an estimated historical cost of about $4 billion. OIG has identified problems in the Department's acquisition and disposition decisions for real property, including funding decisions. These findings contributed to legislation requiring the establishment of a Real Property Advisory Board to act as the arbitrator of disposal or retention of oversized, underutilized, and high-value properties. OIG has completed a review of the activities of the Board, and found that disputed properties are appropriately chosen for the Board's review and recommendations of the Board are based on sufficient information.

At the request of the Under Secretary for Management, OIG is working with the Department to assist in identifying excess, underutilized, and obsolete government-owned and long-term leased real properties worldwide. OIG has conducted limited reviews of real property in the course of its ongoing audits and inspections at overseas posts. Since March 1998, OIG has provided the Department with reviews on 48 posts, and is in the process of completing reviews on another 24 posts. The reviews can be used by the Department to manage the acquisition and disposition of overseas real property assets.

To date, OIG reviews have identified 5 properties as excess and 81 properties underutilized. An example of the latter included a nearly 1-acre unpaved site near the chancery building in Paris used to provide parking for official vehicles and free parking to some embassy employees. According to post officials, there were plans to construct an office building on the site in the mid-1980's, but those plans had been rejected. The Department has no plans to develop this site, and has stated that sale of the property would raise security and operational concerns. OIG reviews also identified 6 properties as obsolete. For example, OIG has identified two obsolete properties at Embassy Harare, requiring immediate Department attention for disposal action.

OIG reviews also noted 29 properties that the Department had previously identified for future development or disposal when local economic conditions become favorable. Examples include properties in Bangkok, Seoul, and Kathmandu.

The Department and overseas posts have recently addressed many real property maintenance and repair issues, in part, due to the work of the OIG. In 1993, OIG recommended that the Department establish a system to identify and monitor the

worldwide maintenance and repair requirements and establish an initial baseline for outstanding maintenance and repair requirements. In response to the recommendation, the Department has established a system to identify and monitor requirements, but has not analyzed the information contained in that system to establish a baseline of maintenance and repair requirements and costs. Future OIG work will evaluate the Department's systems to identify, prioritize, and perform maintenance and repair.

* * *

In conclusion, Mr. Chairman, I have outlined what my office believes are the major management challenges facing the foreign affairs agencies we oversee. While we have focused much of our work in these areas, there are no quick fixes. Indeed, several of these issues have been the subject of repeated OIG recommendations. Overcoming these challenges will require careful and long-term management attention. In some areas, such as addressing security vulnerabilities, additional resources will be required.

I look forward to working with members of this subcommittee in the coming year on many of these issues. I would be pleased to answer any questions you may have.